CLASS 726, INFORMATION SECURITY

SECTION I - CLASS DEFINITION

GENERAL STATEMENT OF THE CLASS SUBJECT MATTER

This class provides, within a computer or digital data processing system, for processes or apparatus for increasing a system s extension of protection of system hardware, software, or data from maliciously caused destruction, unauthorized modification, or unauthorized disclosure.

INFORMATION SECURITY

This class provides for protection of data processing systems, apparatus, and methods as well as protection of information and services. Subject matter included in this class includes security policies, access control, monitoring, scanning data, countermeasures, usage control, and data protection from maliciously caused destruction, unauthorized modification, or unauthorized disclosure. This class also includes protection of hardware, and user protection, e.g., privacy, etc.

SECTION II - REFERENCES TO OTHER CLASSES

SEE OR SEARCH CLASS:

326, Electronic Digital Logic Circuitry, subclass 8 for digital logic circuits acting to disable or prevent access to stored data or designated integrated circuit structure.

340, Communications: Electrical, subclasses 5.2 through 5.74 for authorization control without significant data process features claimed, particularly subclasses 5.22-5.25 for programmable or code learning authorization control; and subclasses 5.8-5.86 for intelligence comparison for authentication.

365, Static Information Storage and Retrieval, subclass 185.04 for floating gate memory device having ability for securing data signal from being erased from memory cells.

380, Cryptography, subclasses 200 through 242 for video with data encryption; subclasses 243-246 for facsimile encryption; subclasses 247-250 for cellular telephone cryptographic authentication; subclass 251 for electronic game using cryptography; subclasses 255-276 for communication using cryptography; subclasses 277-47 for key management; and subclasses 287-53 for electrical signal modification with digital signal handling.

455, Telecommunications, subclass 410 for security or fraud prevention in a radiotelephone system.

704, Data Processing: Speech Signal Processing, Linguistics, Language Translation, and Audio Compression/Decompression, subclass 273 for an application of speech processing in a security system.

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass 18 for security in an electronic cash register or point of sale terminal having password entry mode, and subclass 44 for authorization or authentication in a credit transaction or loan processing system.

708, Electrical Computers: Arithmetic Processing And Calculating, subclass 135 for electrical digital calculating computer with specialized input for security.

710, Electrical Computers and Digital Data Processing Systems: Input/Output, subclasses 36 through 51 for regulating access of peripherals to computers or vice-versa; subclasses 107-125 for regulating access of processors or memories to a bus; and subclasses 200-240 for general purpose access regulating and arbitration.

711, Electrical Computers and Digital Processing Systems: Memory, subclass 150 for regulating access to shared memories, subclasses 163-164 for preventing unauthorized memory access requests.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 150 through 181 for multiple computer communication using cryptography; subclasses 182-186 for system access control based on user identification by cryptography; subclass 187 for computer program modification detection by cryptography; subclass 188 for computer virus detection by cryptography; and subclasses 189-194 for data processing protection using cryptography.

714, Error Detection/Correction and Fault Detection/Recovery, subclasses 1 through 57 for recovering from, locating, or detecting a system fault caused by malicious or unauthorized access (e.g., by virus, etc.).

SECTION III - GLOSSARY

ACCESS CONTROL

The prevention of unauthorized access to resources of a

system or information system, including the prevention of their use in an unauthorized manner.

INFORMATION

Data with meaning concerning a particular act or circumstance in general. Note: May include or consist of graphics or text or numerical or non-numerical values.

MONITORING

Subject matter includes means of watching, tracking, inspecting, analyzing of system or user activity. This includes the auditing of system vulnerabilities and system configuration, assessing the integrity of files within a system, identifying and recognizing patterns that dictate known attacks, analysis of abnormal activity patterns, recognizing user activity in regards to policy violations and operating system audit trail management.

POLICY

Rules for protecting information, services and other data processing resources.

USAGE CONTROL

Subject matter includes means placing restrictions on computer and/or user use of applications

USER PROTECTION/PRIVACY

Subject matter includes means for ensuring the state or integrity of information or data associated with a user.

SUBCLASSES

1 POLICY:
This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus that provide for the administration and management of rules or regulations governing the protection of information, services and other data processing resources involving coordination of more than one security mechanisms among a plurality of entities, resources, or processes.

2 ACCESS CONTROL OR AUTHENTICATION:
This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus for the prevention of unauthorized access to resources of a system or information system, including the manner of identifying and verifying the entity, process, or mechanism requesting access to the resource.

(1) Note. This subclass is directed to access control in information security systems. The concept of access control exists throughout the class. Therefore, a search to a particular concept of access control should consider the related topics in bus access control, memory access control, computer system access control, generic access control, etc.

SEE OR SEARCH THIS CLASS, SUBCLASS:
27, for prevention of unauthorized use of data access control.

SEE OR SEARCH CLASS:
340, Communications: Electrical, subclasses 5.8 through 5.86 for selective electrical communications systems with intelligence comparison for identity authentication.
345, Computer Graphics Processing and Selective Visual Display Systems, subclasses 716 through 726 for operator interface aspects of workgroup data processing environments for plural users or sites.
380, Cryptography, appropriate subclasses for systems employing encrypted user or record actuated authentication, and for digital control or digital computer communication in which an encrypting or decrypting device utilizes a digital signal manipulation technique on the computer signal, and subclasses 247 through 250 for cellular telephone cryptographic authentication.
705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass 18 for an electronic cash register having cryptography; and subclass 44 for a general funds transfer or credit transaction requiring authorization or authentication not including a cryptographic limitation.
707, Data Processing: Database and File Management or Data Structures, subclass 9 for privileged database or file accessing.

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclass 225 for controlling which of plural computers may transfer data via a communications medium.

710, Electrical Computers and Digital Data Processing Systems: Input /Output, subclasses 107 through 125 for bus access regulating.

711, Electrical Computers and Digital Processing Systems: Memory, subclasses 147 through 153 for shared memory access and control, and subclasses 163-164 for access limiting and password use therein.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 155 through 159 for central trusted authority authentication; subclasses 168-181 for particular communication authentication technique; and subclasses 182-186 for system access control based on cryptographic user identification.

3 Network:

This subclass is indented under subclass 2.
Subject matter including means of limiting access to the resources of a system based on a network level.

(1) Note. The network level is computer-to-computer communication.

SEE OR SEARCH CLASS:

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclass 22 controlling which of plural computers may transfer data via a communications medium.

4 Authorization:

This subclass is indented under subclass 3.
Subject matter including permitting the use of rights, privileges, and permissions in a network environment.

SEE OR SEARCH THIS CLASS, SUBCLASS:

18, for stand-alone authorization.

21, for access control or authentication.

5 Credential:

This subclass is indented under subclass 3.
Subject matter including the existence of network data that can be used to establish the claimed identity of a principal including passwords, biometrics.

SEE OR SEARCH CLASS:

382, Image Analysis, subclass 115 for image analysis for personal identification (biometrics).

713, Electrical Computers and Digital Processing Systems: Support, subclass 186 for biometric acquisition.

902, Electronic Funds Transfer, cross-reference art collection 3, for biometric evaluation in electronic funds transfer.

6 Management:

This subclass is indented under subclass 5.
Subject matter including means or steps for administering credentials, including specific techniques for creating the credentials.

SEE OR SEARCH THIS CLASS, SUBCLASS:

18, for stand-alone credential management.

7 Usage:

This subclass is indented under subclass 5.
Subject matter including means or steps for using the credential to establish the identity of the bearer.

SEE OR SEARCH THIS CLASS, SUBCLASS:

20, for stand-alone credential usage.

8 Global (e.g., Single Sign On (SSO), etc.):

This subclass is indented under subclass 5.
Subject matter whereby a single credential can be used to access a plurality of systems or resources.

9 Tokens (e.g., smartcards or dongles, etc.):

This subclass is indented under subclass 5.
Subject matter whereby the credential includes a unique combination of bits used to confer transmit privileges to a computer on a local network.

SEE OR SEARCH THIS CLASS, SUBCLASS:

20, for stand-alone authorization.

SEE OR SEARCH CLASS:

380, Cryptography, subclass 229 for authentication in a video system using a record or token.

705, Data Processing: Financial, Business Practice, Management, or Cost /Price Determination, subclasses 65 through 69 for secure transaction including intelligent token.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 172 through 174 for generic authentication using intelligent token in multiple computer communication.

10 Tickets (e.g., Kerberos or certificates, etc.):

This subclass is indented under subclass 5.

Subject matter whereby the credential includes data used to indicate that the bearer is authorized for access.

SEE OR SEARCH CLASS:

713, Electrical Computers and Digital Processing Systems: Support, subclasses 156 through 158 for computer network certificates, and subclass 175 for generation of a certificate.

11 Firewall:

This subclass is indented under subclass 3.

Subject matter including a device installed between internal (private) networks and outside networks (public) and which protects the internal network from network-based attacks that may originate from the outside and to provide a traffic point where security constraints and audits may be affected.

SEE OR SEARCH CLASS:

370, Multiplex Communications, subclasses 351 through 430 for multiplex communication routing absent cryptography.

705, Data Processing: Financial, Business Practice, Management, or Cost /Price Determination, subclass 79 for cryptographic remote charge determination of a secure transaction including payment switch or gateway.

709, Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring, subclasses 238 through 244 for computer-to-computer data routing.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 153 and 154 for a particular node in cryptographically protected multiple computer communication.

12 Proxy server or gateway:

This subclass is indented under subclass 11.

Subject matter including an intermediate internetworking device that connects one or more networks to another for a specific application.

(1) Note. The gateway runs a process at the request of the client/user and obtains the service of a particular server; hence it works as both a client and a server provider.

13 Packet filtering:

This subclass is indented under subclass 11.

Subject matter including a multi-ported internetworking device that applies a set of rules to each incoming IP packet in order to decide whether it is to be forwarded or dropped.

(1) Note. The filtering usually takes place on information contained in the headers, such as protocol numbers, source or destination addresses/ports, TCP connections, and other options. The filtering may be dynamic or static.

(2) Note. The packet filter may be different and distinct from routers; see note on routers. Routers are internetworking devices that run a custom operating system to transfer packets between two or more physically separated network segments (via the use of routing tables). This device operates at the network level of the OSI model, or the Internet level of the Internet model.

(3) Note. Some routers have a scanning ability and are know as screening routers, effectively becoming a packet-filtering device.

14 Security protocols:
This subclass is indented under subclass 11.
Subject matter including a set of rules, procedures, or conventions governing the format and relative timing of message exchange between two communications terminals to prevent unauthorized intrusion or interference (i.e., attacks).

15 Virtual Private Network or Virtual Terminal Protocol (i.e., VPN or VTP):
This subclass is indented under subclass 14.
Subject matter wherein the protocol is used for a software-defined network offering the appearance, functionality, and usefulness of a dedicated private network or for a terminal that is defined as a standard on the network that can handle diverse terminals.

SEE OR SEARCH CLASS:
370, Multiplex Communications, subclass 351 for a path finding or routing through a switching network or a packet switching network.
379, Telephonic Communications, cross-reference art collection 901 for virtual network or virtual private network for a telephonic device.

16 Stand-alone:
This subclass is indented under subclass 2.
Subject matter wherein the access control or authentication includes the means of limiting access to the resources of a system based on a single computer or end user level.

(1) Note. The end user level is the occupant of the premises who uses the product.

17 Authorization:
This subclass is indented under subclass 16.
Subject matter wherein the access control or authentication includes permitting the use of rights, privileges, and permissions in the stand-alone network environment.

SEE OR SEARCH THIS CLASS, SUBCLASS:
4, for network authorization.
21, for standalone credential management.

18 Credential management:
This subclass is indented under subclass 17.
Subject matter wherein the authorization includes systems, methods, or apparatus for administering information supplied to authenticate a communication.

(1) Note. This subject includes specific techniques for creating the credentials.

SEE OR SEARCH THIS CLASS, SUBCLASS:
6, for network credential management.

19 Credential usage:
This subclass is indented under subclass 17.
Subject matter wherein the authorization includes systems, methods, and apparatus for using information supplied to authenticate a communication to establish the identity of the bearer.

SEE OR SEARCH THIS CLASS, SUBCLASS:
7, for network credential usage.

20 Tokens (e.g., smartcards or dongles, etc.):
This subclass is indented under subclass 17.
Subject matter wherein the authorization includes a unique combination of bits used to confer transmit privileges to a computer on a stand-alone.

SEE OR SEARCH THIS CLASS, SUBCLASS:
9, for network credential tokens.

21 Authorization:
This subclass is indented under subclass 2.
Subject matter wherein access control means includes use of permissions, rights, or privileges.

SEE OR SEARCH THIS CLASS, SUBCLASS:
4, for network authorization.
17, for stand-alone authorization.

22 MONITORING OR SCANNING OF SOFTWARE OR DATA INCLUDING ATTACK PREVENTION:

This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus for ensuring data integrity by scanning of software or data or otherwise monitoring data to prevent or detect attacks.

SEE OR SEARCH CLASS:

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclasses 51 through 54 for usage protection of a distributed data file, and subclass 405 for cost/data protection.

713, Electrical Computers and Digital Processing Systems: Support, subclasses 189 through 194 for data processing protection using cryptography.

717, Data Processing: Software Development, Installation, and Management, 168-173 for software upgrading or updating (including plural version management) and subclasses 174 through 178 for software installation.

23 Intrusion detection:

This subclass is indented under subclass 22. Subject matter comprising means to sense the presence of an intruder.

24 Virus detection:

This subclass is indented under subclass 23. Subject matter wherein the intruder is a virus.

SEE OR SEARCH CLASS:

713, Electrical Computers and Digital Processing Systems: Support, subclasses 150 through 181 for multiple computer communication using cryptography; and subclasses 187 and 188 for software program protection or computer virus detection in combination with data encryption.

25 Vulnerability assessment:

This subclass is indented under subclass 22. Subject matter wherein monitoring or scanning of software or data includes methods or systems to evaluate the defensive capabilities of a system, process, apparatus, or entity against attacks.

(1) Note. The subject matter of this subclass is primarily concerned with keeping out intruders and preventing attacks as opposed to authenticating users.

26 PREVENTION OF UNAUTHORIZED USE OF DATA INCLUDING PREVENTION OF PIRACY, PRIVACY VIOLATIONS, OR UNAUTHORIZED DATA MODIFICATION:

This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus for prohibiting any impersonation, unauthorized browsing, falsification or theft of data, or alteration of data not consistent with defined security policy.

SEE OR SEARCH CLASS:

380, Cryptography, subclasses 200 through 242 for video with data encryption; subclasses 243-246 for facsimile encryption; subclasses 247-250 for cellular telephone cryptographic authentication; subclass 251 for electronic game using cryptography; subclasses 255-276 for communication using cryptography; subclasses 277-47 for key management; and subclasses 287-53 for electrical signal modification with digital signal handling.

399, Electrophotography, subclass 366 for document handling of unauthorized copy prevention.

455, Telecommunications, subclass 26.1 for subject matter which blocks access a signal source or otherwise limits usage of modulated carrier equipment.

700, Data Processing: Generic Control Systems or Specific Applications, subclasses 225 through 227 for data processing article handling system having identification code, and subclass 237 for an operator or payment initiated dispensing or ending data processing system having password or PIN authorization.

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass 18 for security in an electronic cash register or point of sale terminal having password entry mode; subclasses 57 and 58 for preventing access to or copying of stored information in a distributed data file.

711, Electrical Computers and Digital Processing Systems: Memory, subclass 164 for memory access requiring authorization code information (e.g., password or key other than encryption key, etc.).

713, Electrical Computers and Digital Processing Systems: Support, subclass 187 for computer program modification detection by cryptography.

714, Error Detection/Correction and Fault Detection /Recovery, subclasses 763 through 773 for memory access block coding, and subclass 805 for storage accessing error/fault detection techniques.

27 Access control:
This subclass is indented under subclass 26. Subject matter comprising means to control data tampering by limiting access to authorized entities or processes.

SEE OR SEARCH THIS CLASS, SUBCLASS:

2, for general access control or authentication of information security.

28 By authorizing user:
This subclass is indented under subclass 27. Subject matter wherein the access control includes means to limit access by an authorized user.

29 By authorizing client:
This subclass is indented under subclass 27. Subject matter wherein the access control includes means to limit access to an authorized client.

30 By authorizing data:
This subclass is indented under subclass 27. Subject matter wherein the access control includes means to limit access by the data to be used.

31 Limitations on number or amount of copies:
This subclass is indented under subclass 26. Subject matter wherein the prevention of unauthorized use of data includes means to limit number or amount of electronic copies of the data that can be made.

32 Copy detection:
This subclass is indented under subclass 26. Subject matter including means to prevent unauthorized use by detecting electronic copying of data.

SEE OR SEARCH CLASS:

380, Cryptography, subclasses 201 through 204 for copy protection or prevention of a video signal.

399, Electrophotography, subclass 366 for document handling of unauthorized copy prevention.

705, Data Processing: Financial, Business Practice, Management, or Cost/Price Determination, subclass 57 for copy protection or prevention.

33 Copy inactivation:
This subclass is indented under subclass 26. Subject matter including means to prevent unauthorized use by rendering an electronic copy inactive unless access is authorized.

34 PROTECTION OF HARDWARE:
This subclass is indented under the class definition. Subject matter comprising systems, methods, and apparatus used for safeguarding physical equipment used in data processing.

SEE OR SEARCH CLASS:

49, Movable or Removable Closures, subclasses 13 and 14 for closure condition indicator.

70, Locks, subclasses 432 through 441 and Digest 49 for locks with indicator or alarm.

109, Safes, Bank Protection, or a Related Device, subclass 21 for bank protection device with alarm or indicator; subclass 31 for art device combined with fluent material distributing, generating device for alarm or indicator; and subclass 38 for combined art device with alarm or indicator.

116, Signals and Indicators, subclass 6 for burglar alarm and subclass 33 for vehicle theft prevention.

340, Communications: Electrical, subclasses 287 through 309 for a signal box alarm arrangement, particularly subclass 288 for alarm transmission over a power line; subclasses 426.1-426.36 for vehicle alarms or indication of burglary or unauthorized use; and subclasses 541-567 for an intrusion responsive indicator or alarm.

348, Television, subclass 152 for intrusion detection by a television camera.

361, Electricity: Electrical Systems and Devices, appropriate subclasses for safety and protection of systems and devices.

379, Telephonic Communications, subclasses 37 through 51 for emergency or alarm communications (e.g., watchman's circuit, etc.), particularly subclass 39 for subject matter responsive to sense nonsystem condition, external to the telephone system, and subclasses 106.01-106.11 for remote condition indication, other than an emergency or alarm condition, over a telephone line.

35 Theft prevention:

This subclass is indented under subclass 34. Subject matter wherein the protection of hardware includes means to prevent unauthorized removal of hardware.

36 Via power supply:

This subclass is indented under subclass 34. Subject matter wherein the protection of hardware includes means for protecting hardware by interruption of power supply.

SEE OR SEARCH CLASS:

713, Electrical Computers and Digital Processing Systems: Support, subclasses 300 through 340 for computer power control, in general.

END